

State of Arizona
Senate
Forty-eighth Legislature
First Regular Session
2007

Senate Engrossed
FILED
JANICE K. BREWER
SECRETARY OF STATE

CHAPTER 23

SENATE BILL 1042

AN ACT

AMENDING SECTION 44-7501, ARIZONA REVISED STATUTES; RELATING TO NOTIFICATION
FOR COMPROMISED PERSONAL INFORMATION.

(TEXT OF BILL BEGINS ON NEXT PAGE)

1 Be it enacted by the Legislature of the State of Arizona:

2 Section 1. Section 44-7501, Arizona Revised Statutes, is amended to
3 read:

4 44-7501. Notification of breach of security system;
5 enforcement; civil penalty; preemption; exceptions;
6 definitions

7 A. When a person that conducts business in this state and that owns or
8 licenses unencrypted computerized data that includes personal information
9 becomes aware of an incident of unauthorized acquisition and access to
10 unencrypted or unredacted computerized data that includes an individual's
11 personal information, the person shall conduct a reasonable investigation to
12 promptly determine if there has been a breach of the security system. If the
13 investigation results in a determination that there has been a breach in the
14 security system, the person shall notify the individuals affected. The
15 notice shall be made in the most expedient manner possible and without
16 unreasonable delay subject to the needs of law enforcement as provided in
17 subsection C of this section and any measures necessary to determine the
18 nature and scope of the breach, to identify the individuals affected or to
19 restore the reasonable integrity of the data system.

20 B. A person that maintains unencrypted computerized data that includes
21 personal information that the person does not own shall notify and cooperate
22 with the owner or the licensee of the information of any breach of the
23 security of the system following discovery of the breach without unreasonable
24 delay. Cooperation shall include sharing information relevant to the breach
25 of the security of the system with the owner or licensee. The person that
26 owns or licenses the computerized data shall provide notice to the individual
27 pursuant to this section. The person that maintained the data under an
28 agreement with the owner or licensee is not required to provide notice to the
29 individual pursuant to this section unless the agreement stipulates
30 otherwise.

31 C. The notification required by subsection A of this section may be
32 delayed if a law enforcement agency advises the person that the notification
33 will impede a criminal investigation. The person shall make the notification
34 after the law enforcement agency determines that it will not compromise the
35 investigation.

36 D. The disclosure required by subsection A of this section shall be
37 provided by one of the following methods:

38 1. Written notice.

39 2. Electronic notice if the person's primary method of communication
40 with the individual is by electronic means or is consistent with the
41 provisions regarding electronic records and signatures set forth in the
42 electronic signatures in global and national commerce act (P.L. 106-229; 114
43 Stat. 464; 15 United States Code section 7001).

44 3. Telephonic notice.

1 4. Substitute notice if the person demonstrates that the cost of
2 providing notice pursuant to paragraph 1, 2 or 3 of this subsection would
3 exceed fifty thousand dollars or that the affected class of subject
4 individuals to be notified exceeds one hundred thousand persons, or the
5 person does not have sufficient contact information. Substitute notice shall
6 consist of all of the following:

7 (a) Electronic mail notice if the person has electronic mail addresses
8 for the individuals subject to the notice.

9 (b) Conspicuous posting of the notice on the web site of the person if
10 the person maintains one.

11 (c) Notification to major statewide media.

12 E. A person who maintains the person's own notification procedures as
13 part of an information security policy for the treatment of personal
14 information and is otherwise consistent with the requirements of this section
15 shall be deemed to be in compliance with the notification requirements of
16 this section if the person notifies subject individuals in accordance with
17 the person's policies if a breach of the security system occurs.

18 F. A person that complies with the notification requirements or
19 security breach procedures pursuant to the rules, regulations, procedures,
20 guidance or guidelines established by the person's primary or functional
21 federal regulator is deemed to be in compliance with this section.

22 G. A person is not required to disclose a breach of the security of
23 the system if the person or a law enforcement agency, after a reasonable
24 investigation, determines that a breach of the security of the system has not
25 occurred or is not reasonably likely to occur.

26 H. This section may only be enforced by the attorney general. The
27 attorney general may bring an action to obtain actual damages for a wilful
28 and knowing violation of this section and a civil penalty not to exceed ten
29 thousand dollars per breach of the security of the system or series of
30 breaches of a similar nature that are discovered in a single investigation.

31 I. The state legislature determines that security system breach
32 notification is a matter of statewide concern. The power to regulate
33 security breach notification is preempted by this state and this section
34 shall supersede and preempt all municipal and county laws, charters,
35 ordinances and rules relating to issues regulated by this chapter.

36 J. This section does not apply to either of the following:

37 1. A person subject to title V of the Gramm-Leach-Bliley act of 1999
38 (P.L. 106-102; 113 Stat. 1338; 15 United States Code sections 6801 through
39 6809).

40 2. Covered entities as defined under regulations implementing the
41 health insurance portability and accountability act, 45 Code of Federal
42 Regulations section 160.103 (1996).

43 K. ~~A law enforcement agency~~ THE DEPARTMENT OF PUBLIC SAFETY, A COUNTY
44 SHERIFF'S DEPARTMENT, A MUNICIPAL POLICE DEPARTMENT, a prosecution agency and
45 a court shall create and maintain an information security policy that

1 includes notification procedures for a breach of the security system of the
2 ~~law enforcement agency~~ DEPARTMENT OF PUBLIC SAFETY, THE COUNTY SHERIFF'S
3 DEPARTMENT, THE MUNICIPAL POLICE DEPARTMENT, the prosecuting agency or the
4 court.

5 L. For the purposes of this section:

6 1. "Breach", "breach of the security of the system", "breach of the
7 security system" or "security breach" means an unauthorized acquisition of
8 and access to unencrypted or unredacted computerized data that materially
9 compromises the security or confidentiality of personal information
10 maintained by a person as part of a database of personal information
11 regarding multiple individuals and that causes or is reasonably likely to
12 cause substantial economic loss to an individual. Good faith acquisition of
13 personal information by an employee or agent of the person for the purposes
14 of the person is not a breach of the security system if the personal
15 information is not used for a purpose unrelated to the person or subject to
16 further wilful unauthorized disclosure.

17 2. "Court" means the supreme court, court of appeals, superior court,
18 courts inferior to the superior court and justice courts.

19 3. "Encrypted" means use of an algorithmic process to transform data
20 into a form in which the data is rendered unreadable or unusable without use
21 of a confidential process or key.

22 4. "Individual" means a person that is a resident of this state as
23 determined by a principal mailing address in this state as reflected in the
24 records of the person conducting business in this state at the time of the
25 breach.

26 5. ~~"Law enforcement agency" means the department of public safety,~~
27 ~~county sheriff departments or municipal police departments.~~

28 5. "Person" means a natural person, corporation, business trust,
29 estate, trust, partnership, association, joint venture, government,
30 governmental subdivision or agency or any other legal or commercial
31 entity. Person does not include ~~a law enforcement agency~~ THE DEPARTMENT OF
32 PUBLIC SAFETY, A COUNTY SHERIFF'S DEPARTMENT, A MUNICIPAL POLICE DEPARTMENT,
33 a prosecution agency or a court.

34 6. "Personal information":

35 (a) Means an individual's first name or first initial and last name in
36 combination with any one or more of the following data elements, when the
37 data element is not encrypted, redacted or secured by any other method
38 rendering the element unreadable or unusable:

39 (i) The individual's social security number.

40 (ii) The individual's number on a driver license issued pursuant to
41 section 28-3166 or number on a nonoperating identification license issued
42 pursuant to section 28-3165.

43 (iii) The individual's financial account number or credit or debit
44 card number in combination with any required security code, access code or
45 password that would permit access to the individual's financial account.

1 (b) Does not include publicly available information that is lawfully
2 made available to the general public from federal, state or local government
3 records or widely distributed media.

4 ~~8-~~ 7. "Prosecution agency" means the attorney general, any county
5 attorney or any municipal prosecutor.

6 ~~9-~~ 8. "Redact" means alter or truncate data such that no more than
7 the last four digits of a social security number, driver license number,
8 nonoperating identification license number, financial account number or
9 credit or debit card number is accessible as part of the personal
10 information.

APPROVED BY THE GOVERNOR APRIL 10, 2007.

FILED IN THE OFFICE OF THE SECRETARY OF STATE APRIL 11, 2007.